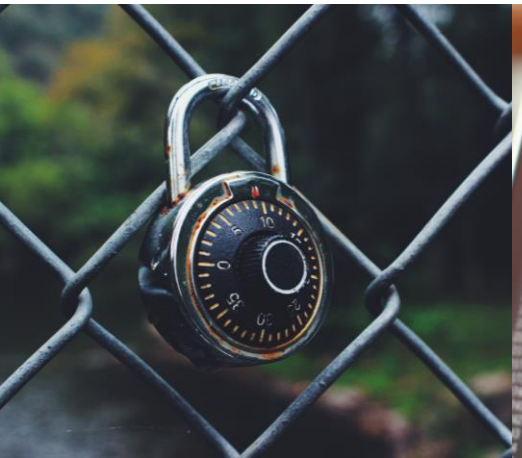
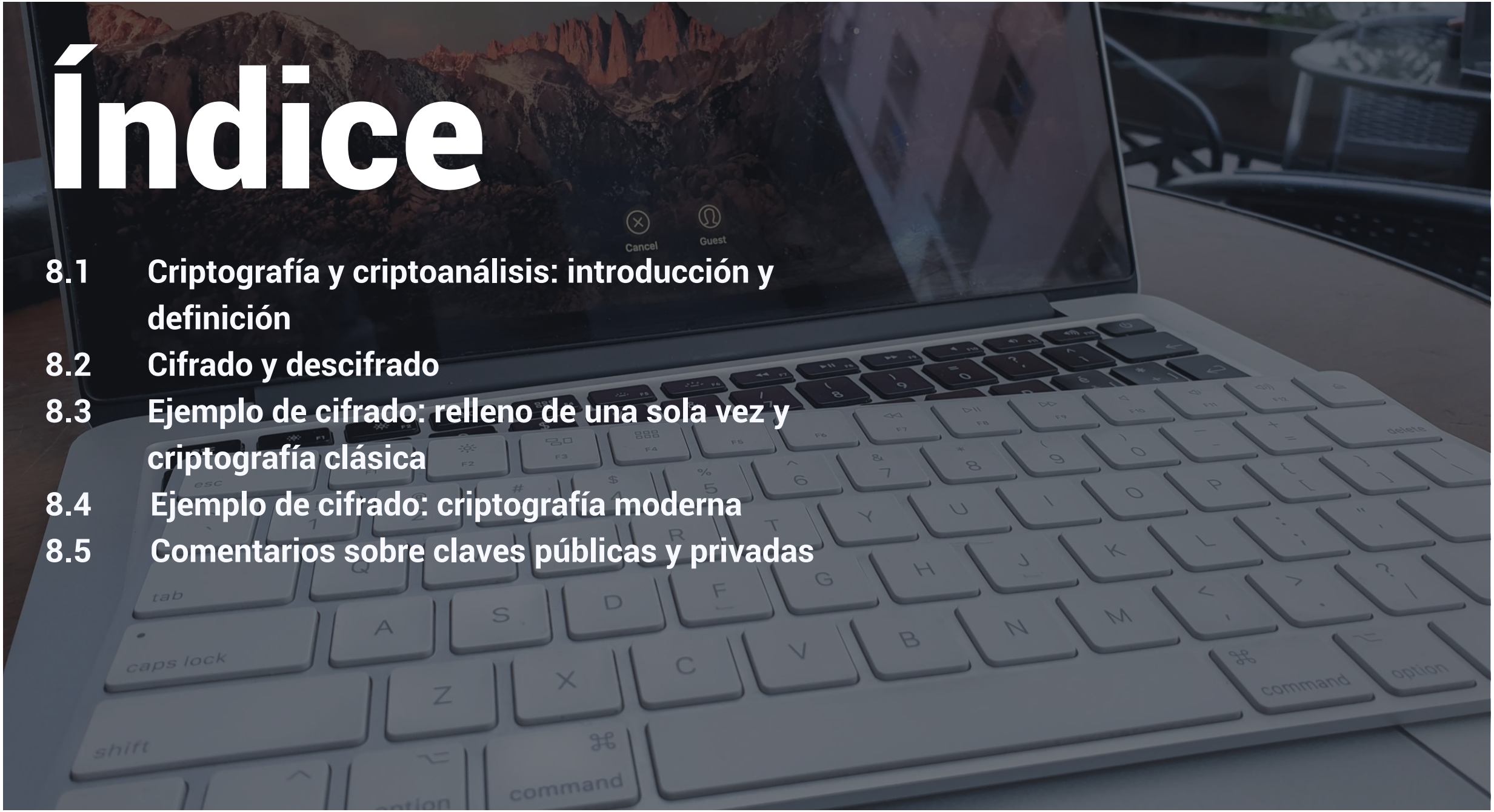
8. Criptografía y criptoanálisis

Proceso

88%




Índice



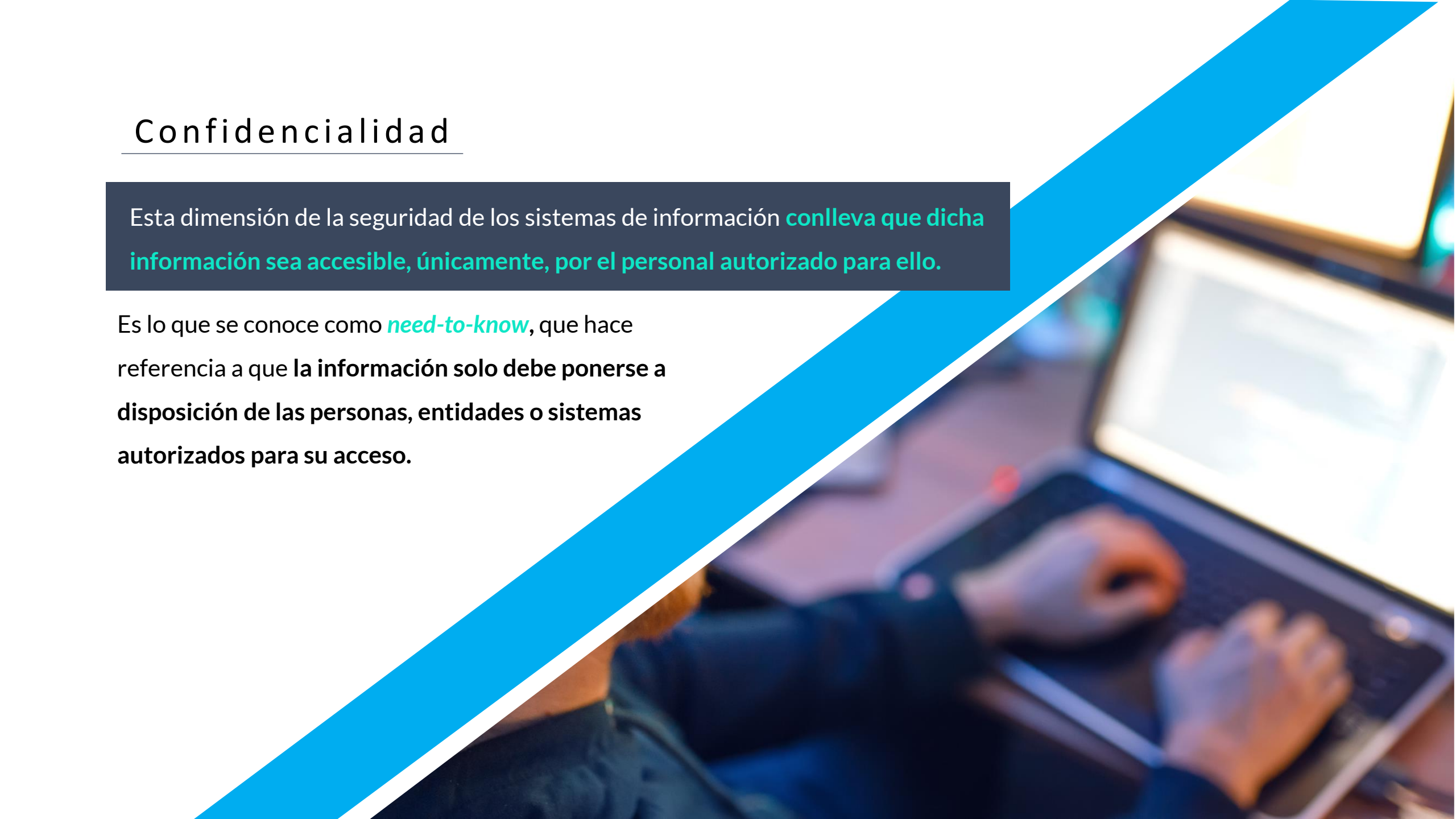
8.1. CRIPTOGRAFÍA Y CRIPTOANÁLISIS


Conceptos básicos
Haz clic sobre la pantalla
MacBook Pro

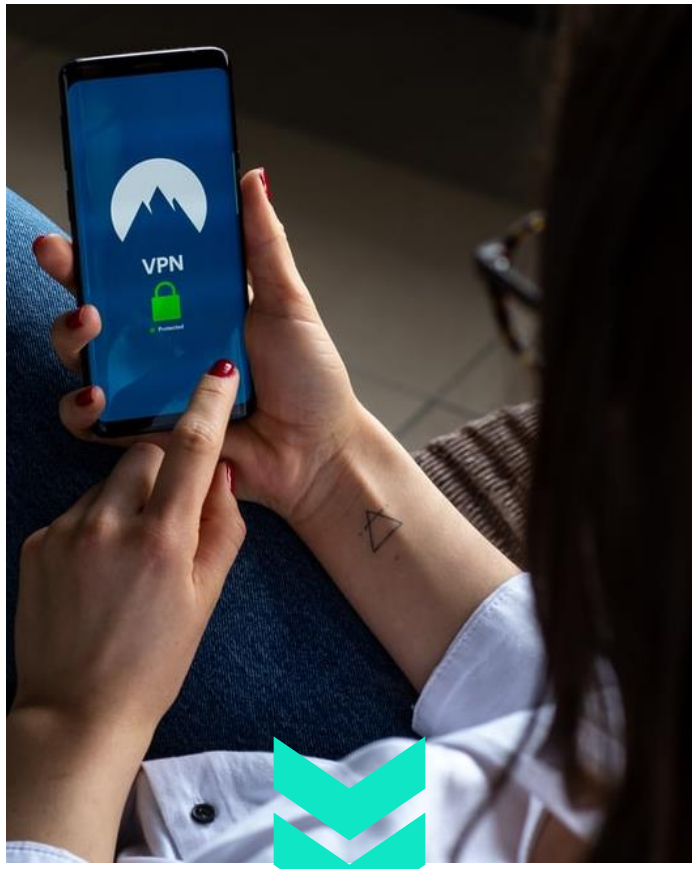
Confidencialidad

Esta dimensión de la seguridad de los sistemas de información **conlleva que dicha información sea accesible, únicamente, por el personal autorizado para ello.**

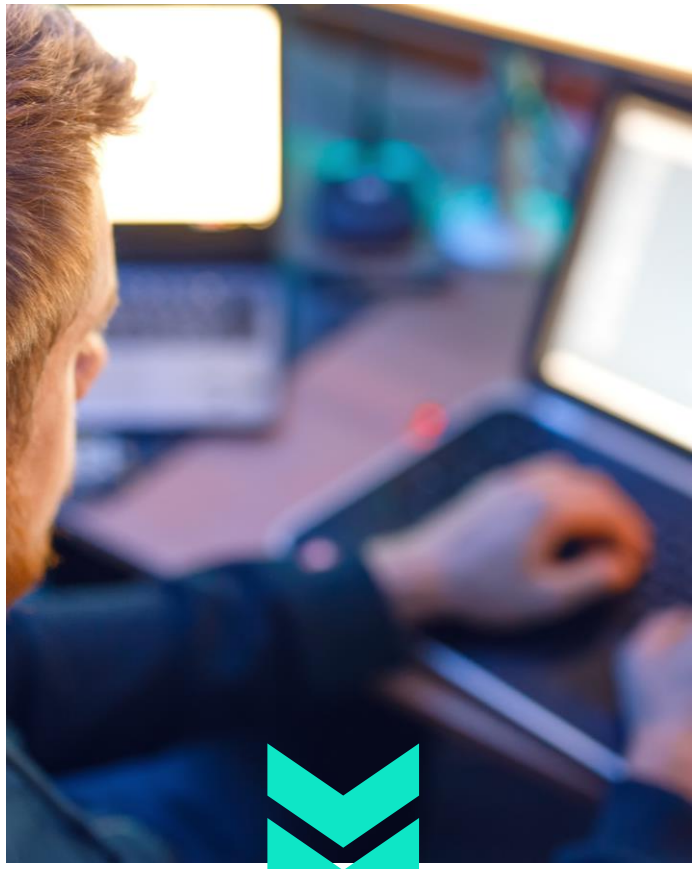
Es lo que se conoce como ***need-to-know***, que hace referencia a que **la información solo debe ponerse a disposición de las personas, entidades o sistemas autorizados para su acceso.**



Podemos poner varios ejemplos de falta de confidencialidad en un sistema:



Robo de información confidencial a través de internet.



Divulgación no autorizada de dicha **información confidencial a través de redes sociales.**

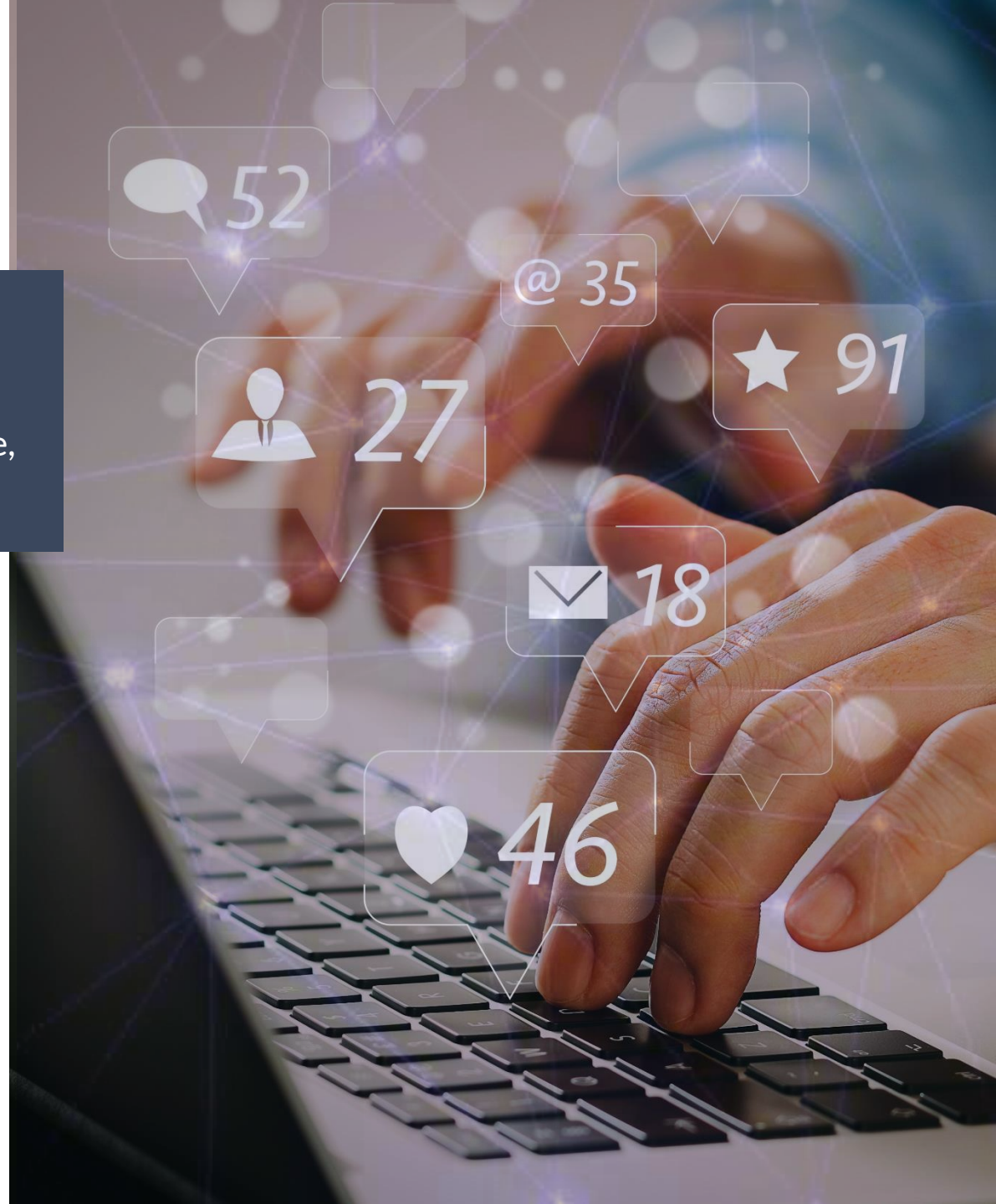
Acceso por parte de **un empleado sin permisos asignados.**

Haz clic sobre las imágenes

Integridad

Este segundo pilar de la seguridad de los sistemas de información hace referencia a que **la información sea correcta y esté libre de modificaciones y errores**, ya que, si no fuese así, podríamos tomar decisiones erróneas.

La información podría ser alterada intencionalmente como, por ejemplo, la modificación de un informe de ventas por parte de un empleado, ya sea malintencionado o por un error humano.



Disponibilidad

La información debe **ser accesible** cuando sea necesaria.

Algún ejemplo práctico sería la imposibilidad de acceder al email corporativo debido a errores de configuración o, incluso, cuando el sistema se cae.

Haz clic para seguir el recorrido

No repudio

Ninguna de las partes involucradas en una operación podrá negar haber enviado o recibido información, es decir, esta acción constituye la **garantía de la identidad de las partes.**

Autenticación

Garantizar el acceso a recursos de la organización, **únicamente, a las personas autorizadas** para ello, se consigue a través de la autenticación de la identidad del usuario, siendo además la única garantía de que un interlocutor es realmente quien dice ser.

Ahora ya estás preparado para descubrir cuáles son las mejores maneras de mantener a salvo la información de nuestra empresa

https://player.vimeo.com/video/338814068?h=5064fac028

Según el vídeo, para evitar el robo de información una solución es ocultar los datos sensibles con **métodos** como:

El encriptado o cifrado

Según el vídeo, para evitar el robo de información una solución es ocultar los datos sensibles con **métodos** como:

El encriptado o cifrado

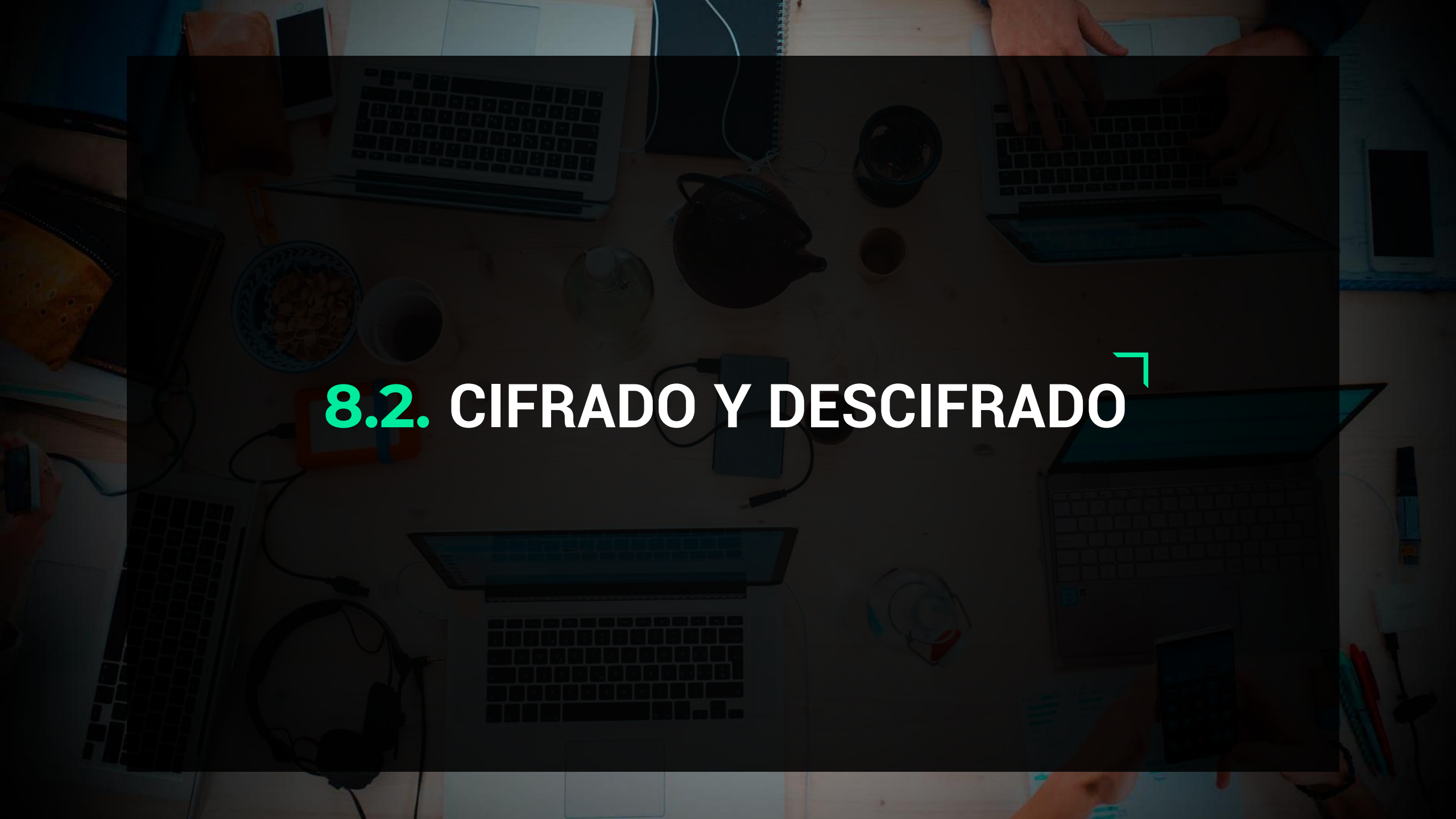
La codificación

Según el vídeo, para evitar el robo de información una solución es ocultar los datos sensibles con **métodos** como:

El encriptado o cifrado

La codificación

Los certificados de seguridad



8.2. CIFRADO Y DESCIFRADO

El encriptado o cifrado

La técnica del cifrado es un método por el que, a través de un algoritmo, se consigue una bidireccionalidad con una clave.

¿Qué significa esto?

Solamente las personas que tengan acceso a la clave podrán entrar y manipular el contenido original, lo que le da un plus de fiabilidad y seguridad.

Dos tipos principales de cifrado

Simétrico

Asimétrico

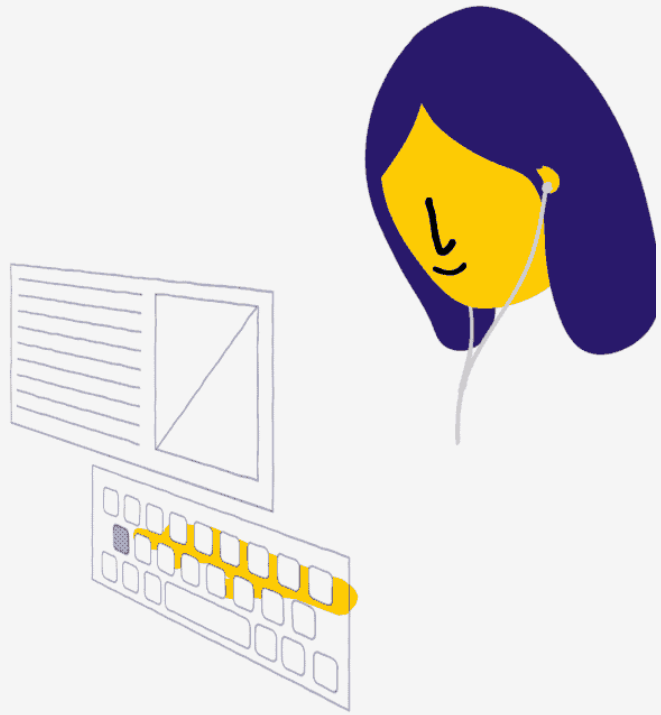
Haz clic sobre el primer botón

Simétrico

En el **cifrado simétrico** la clave secreta o compartida entre el emisor y el receptor **sirve tanto para cifrar como para descifrar el mensaje.**

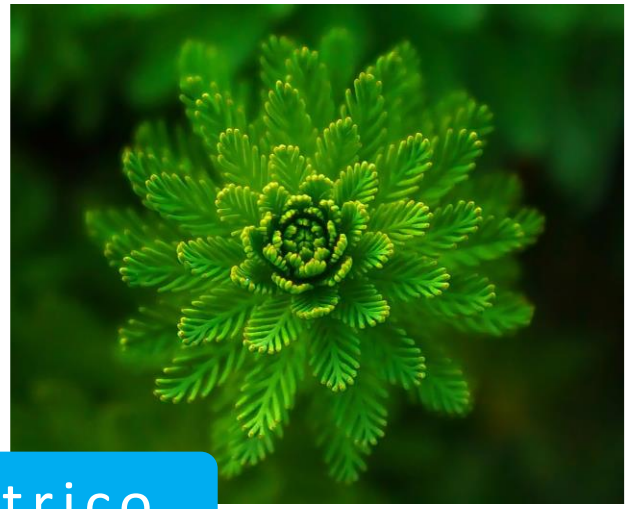
Se trata del **algoritmo más usado**, debido a la rapidez que ofrece a la hora de computar. Es por eso que se utiliza con asiduidad a la hora de cifrar grandes cantidades de información por canales que no destacan por ofrecer demasiada seguridad.

Garantiza, además, la **confidencialidad** de la información.



Ver esquema del cifrado simétrico

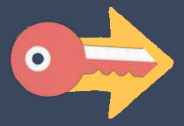
Haz clic sobre el botón

Simétrico


Se cifra con la clave

Se envía

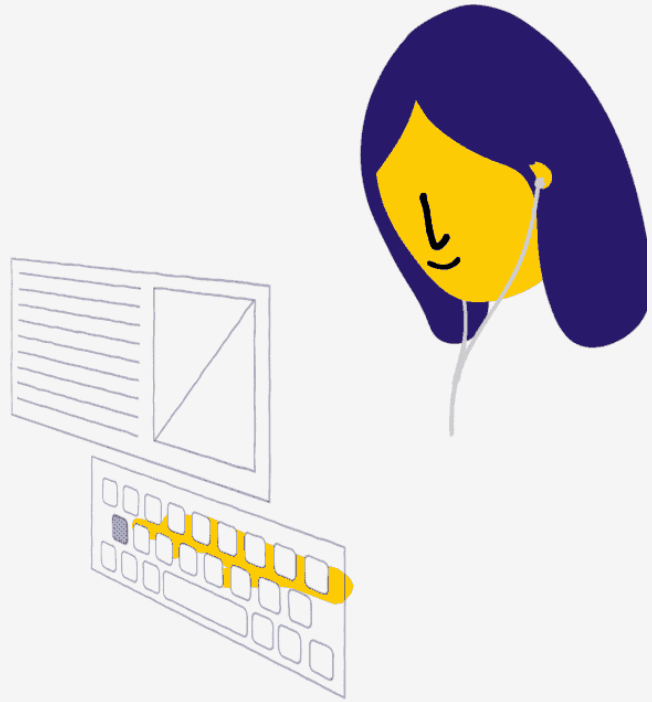
Se descifra con la clave

Asimétrico

En el cifrado asimétrico existen dos claves públicas y privadas, tanto para el destinatario como para el emisor. Esto significa que el mensaje que haya sido cifrado con una clave privada solo podrá ser descifrada con la pública, y viceversa.

Además, mientras que la privada se almacena de forma segura, la pública es compartida explícitamente.

Este tipo de cifrado es mucho más **complejo y caro** que el simétrico, por lo que suele ser usado en transformaciones de pequeñas cantidades de información. Es por ello que **garantiza e incrementa la confidencialidad del mensaje**.



Ver esquema del cifrado asimétrico

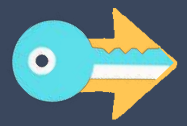
Haz clic sobre el botón



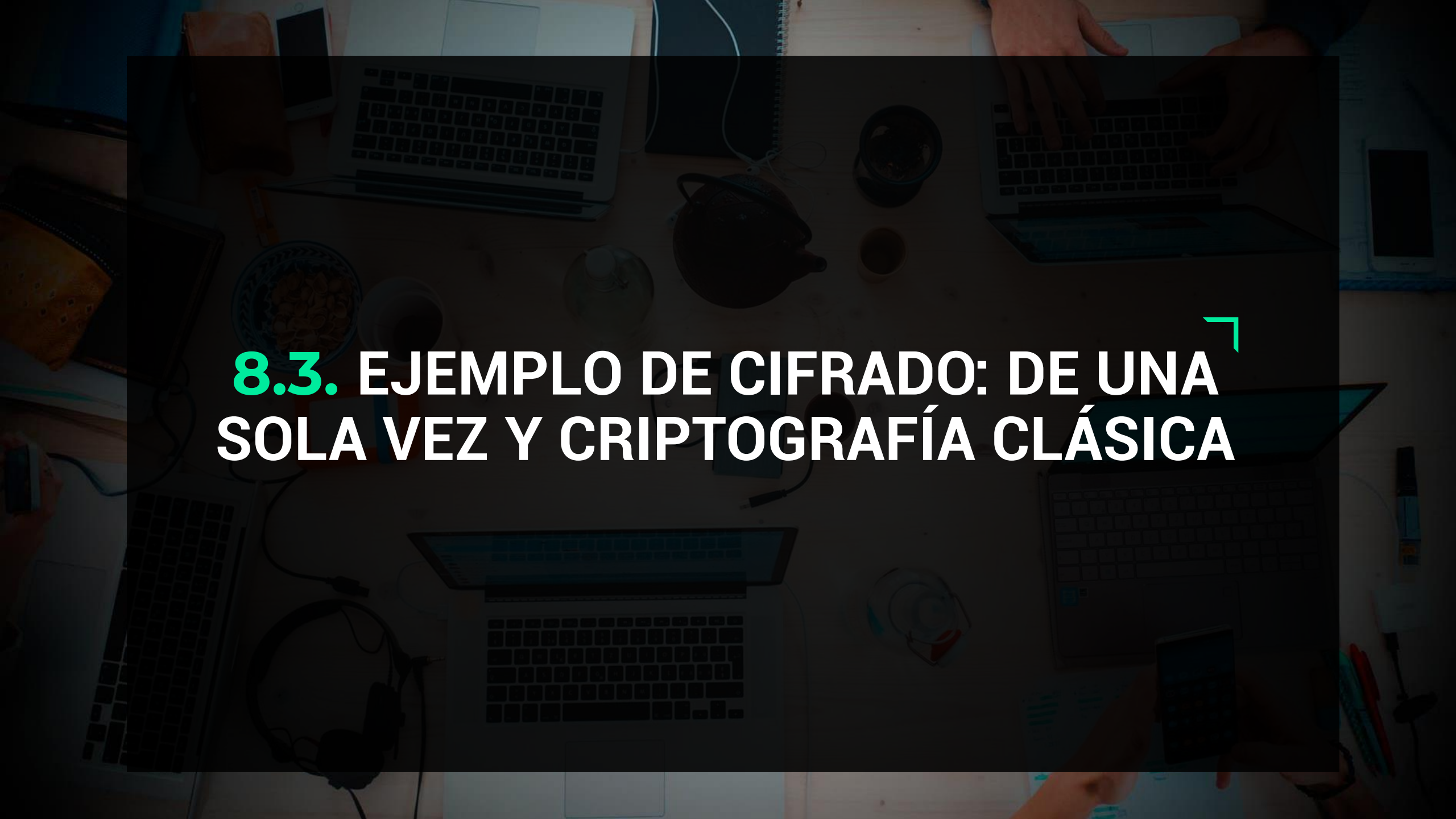

Asimétrico

Andrea cifra con la clave pública de Bruno

Se envía

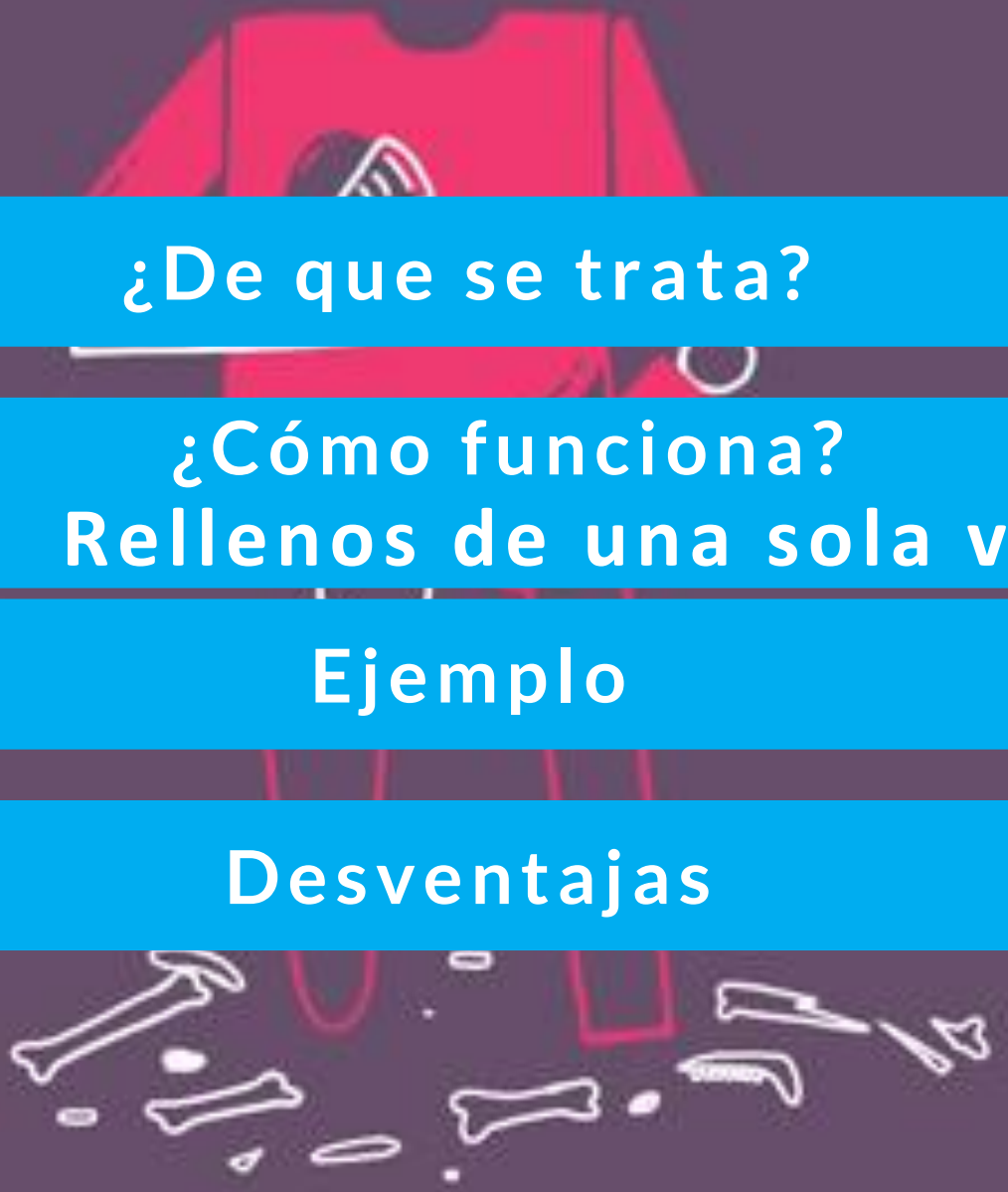



Bruno descifra con su clave privada



8.3. EJEMPLO DE CIFRADO: DE UNA SOLA VEZ Y CRIPTOGRAFÍA CLÁSICA

Haz clic sobre el botón



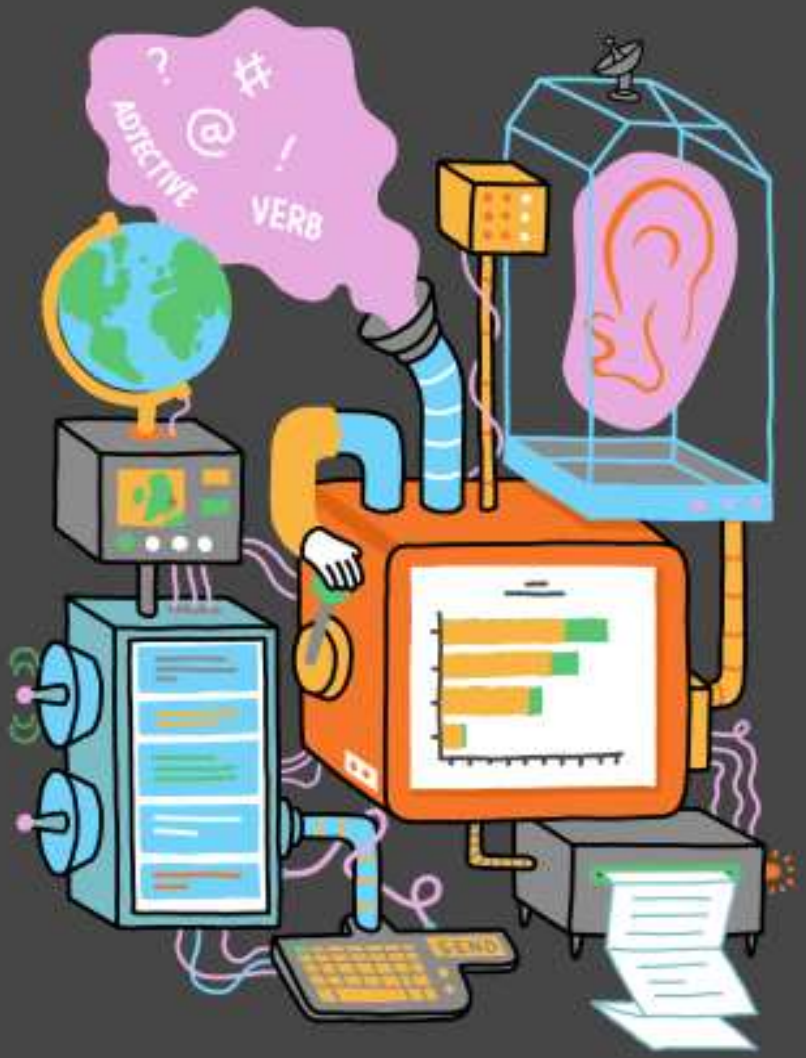
¿De que se trata?

¿Cómo funciona?
Rellenos de una sola vez

Ejemplo

Desventajas

Haz clic en el primer botón

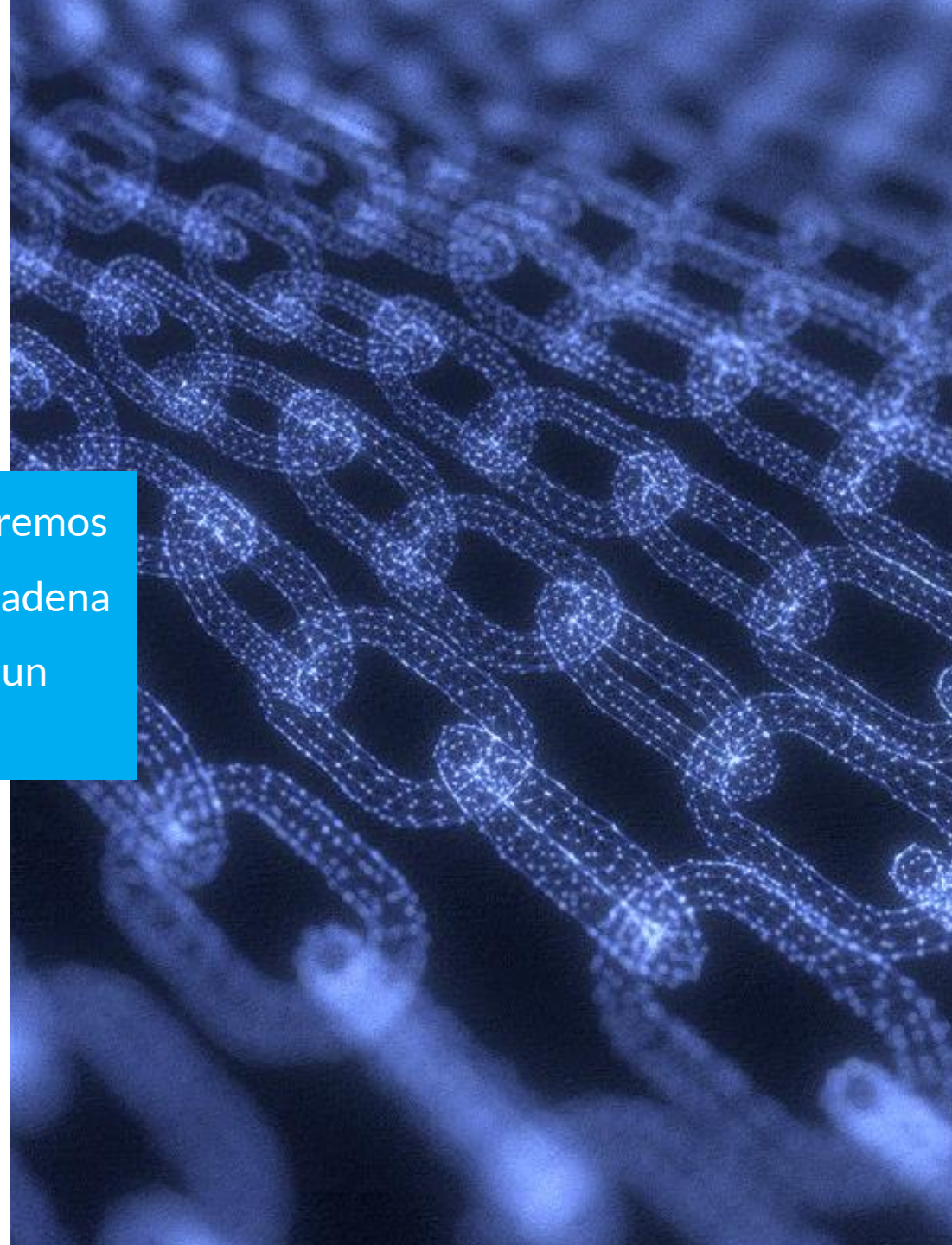


¿De qué se trata?

Se trata de cifrados extremadamente seguros y su construcción, además, puede ser realizada de una forma altamente sencilla.

¿Cómo funciona?

Se escoge totalmente al azar una cadena de bits que utilizaremos a modo de clave. Tras esto, convertiremos el texto en una cadena de bits representados mediante ASCII, por ejemplo, que es un código de caracteres que se basa en el alfabeto latino.



Ejemplo

Se escoge una cadena como clave secreta, por ejemplo, en el lugar de la Mancha de cuyo nombre… y se va aplicando la función XOR sobre el texto normal a cifrar bit a bit.

Texto normal o mensaje P= “texto cifrado”

Cadena de cifrado “En un lugar de la Mancha de cuyo nombre…”

Texto original	t	e	x	t	o		c	i	f	r	a	d	o
Codificación ASCII (hex)	74	65	78	74	6F	20	63	69	66	72	61	64	6F
Cadena de cifrado	E	n		u	n		l	u	g	a	r		d
Codificación ASCII (hex)	45	6E	20	75	6E	20	6C	75	67	61	72	20	64
Codficación cifrada (hex)	31	0B	58	01	01	00	1C	01	13	13	13	44	08

0x74 XOR 0x45=0111 0100 XOR 0100 0101= 0011 0001= 0x31

Para el descifrado, simplemente volvemos a aplicar con XOR la misma cadena de cifrado

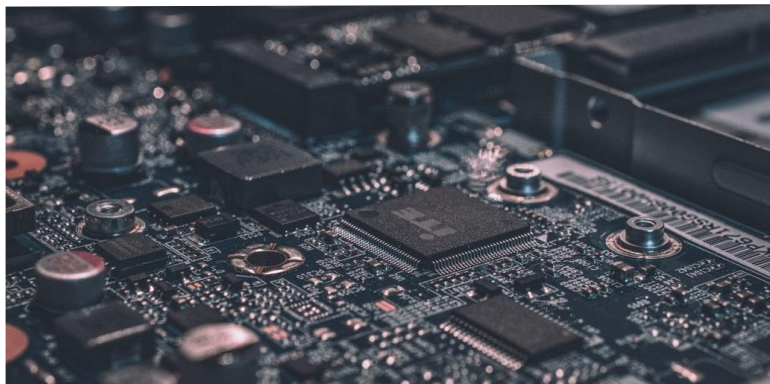
Desventajas

A pesar de su **alta seguridad**, cuenta con una serie de desventajas:

La clave **no puede ser memorizada**, lo que hace que se deba apuntar una copia y llevarla con nosotros.

Los datos que permite **están limitados** a la cantidad de la que dispongamos en la clave.

Lo altamente susceptible que es el método a la **pérdida o inserción de caracteres**. El transmisor y el receptor necesitan, por lo tanto, de una alta sincronía.



Criptografía clásica

Haz clic en el botón

Criptografía clásica

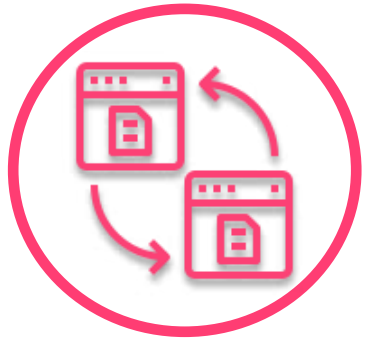
Para explicarla tendríamos que acudir a los sistemas de cifrado que se utilizaban antes de 1939, es decir, cuando empezaron a conformarse los prime ordenadores.

La **criptografía clásica** cimenta en algoritmos sencillos y claves largas para conservar y aumentar la seguridad.

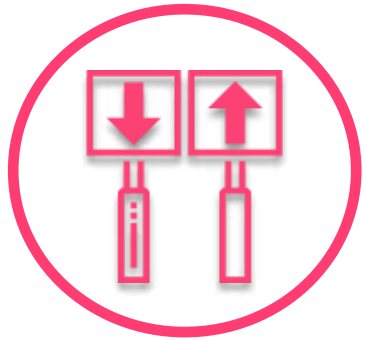
Para explicarla tendríamos que acudir a los sistemas de cifrado que se utilizaban antes de 1939, es decir, cuando empezaron a conformarse los primeros ordenadores.

La **criptografía clásica** se cimenta en algoritmos sencillos y claves largas para conservar y aumentar la seguridad.

Hay dos tipos



Cifrado por sustitución



Cifrado por transposición

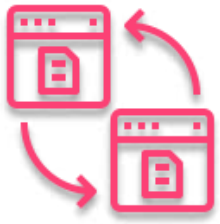
Haz clic en el primer círculo

Cifrado por sustitución

Sustituye cada letra o frase por otras letras o frases con la intención de **encubrirla** y que nadie pueda saber su origen. Sin embargo, cabe destacar que en este cifrado las letras conservan la jerarquía de los símbolos del escrito normal.

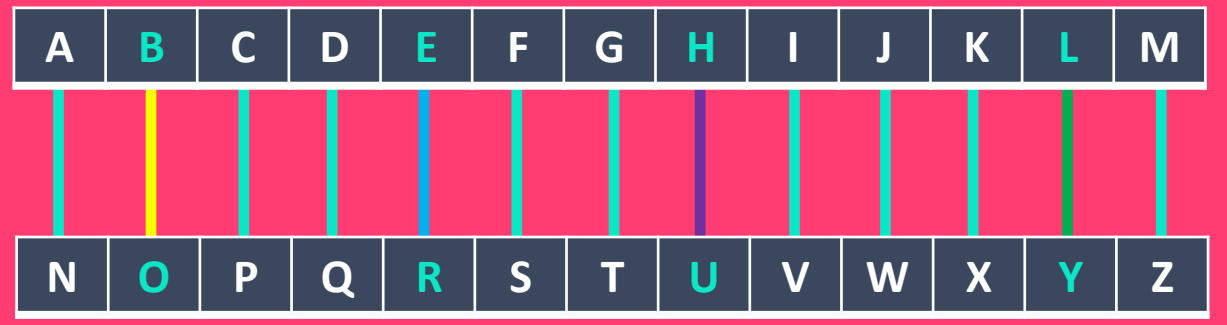
Ejemplo

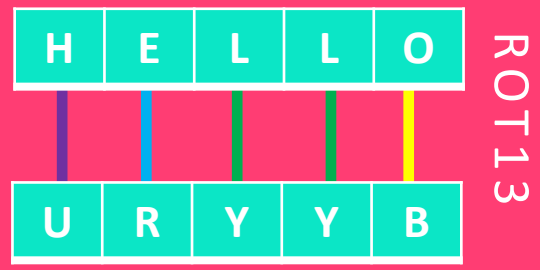
Haz clic en el botón para abrir el ejemplo



Ejemplo

Destacan el cifrado de César o los modelos de cifrado monoalfabéticos, entre otros.



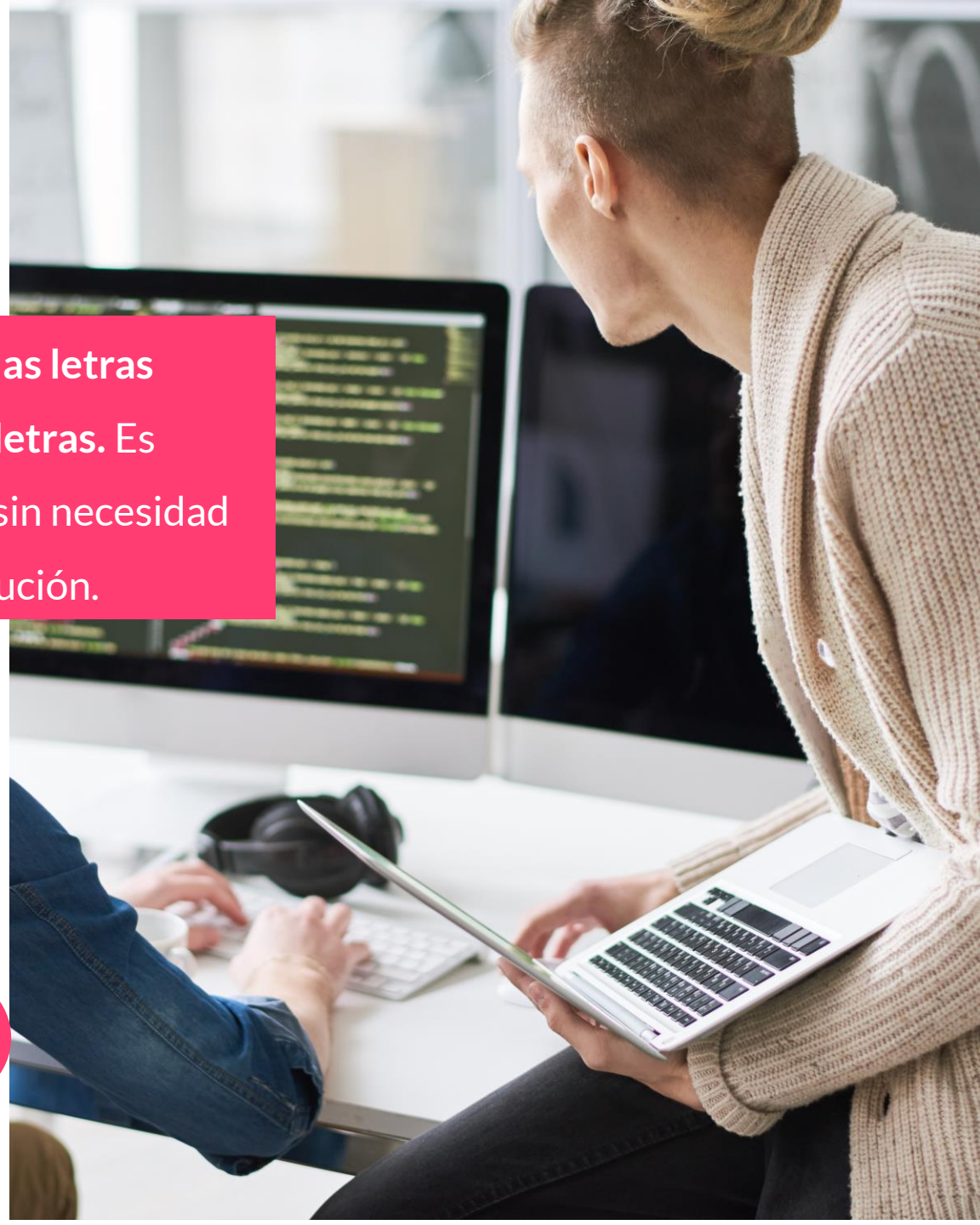


Ejemplo

Haz clic en el botón para cerrar el ejemplo

Cifrado por transposición

La particularidad de este cifrado es que **reordenan las letras acorde a una palabra clave en la que no se repiten letras.** Es decir, se trata de una forma de **reordenar** las letras sin necesidad de disfrazarlas, como sí lo hacía el cifrado por sustitución.



Ejemplo

Haz clic en el botón para abrir el ejemplo.

Ejemplo

Destaca la transposición de columnas.

El texto se escribe fila a fila y se envía leyéndola de columna en columna

Introducción del texto en claro

Extracción del cifrado

E	S	T	E	E	S
U	N	E	J	E	M
P	L	O	D	E	T
R	A	N	S	P	O
S	I	C	I	O	N

C: EUPRS SNLAI TEONC EJDSI EEEPO SMTON

Ejemplo

Haz clic en el botón para cerrar el ejemplo.

8.4. EJEMPLO DE CIFRADO: CRIPTOGRAFÍA MODERNA

Criptografía moderna

Haz clic en el botón

Presente

La **criptografía moderna** mantiene la misma base que la tradicional (en la que se encuentran la transposición y la sustitución), lo cierto es que su **orientación es distinta.**

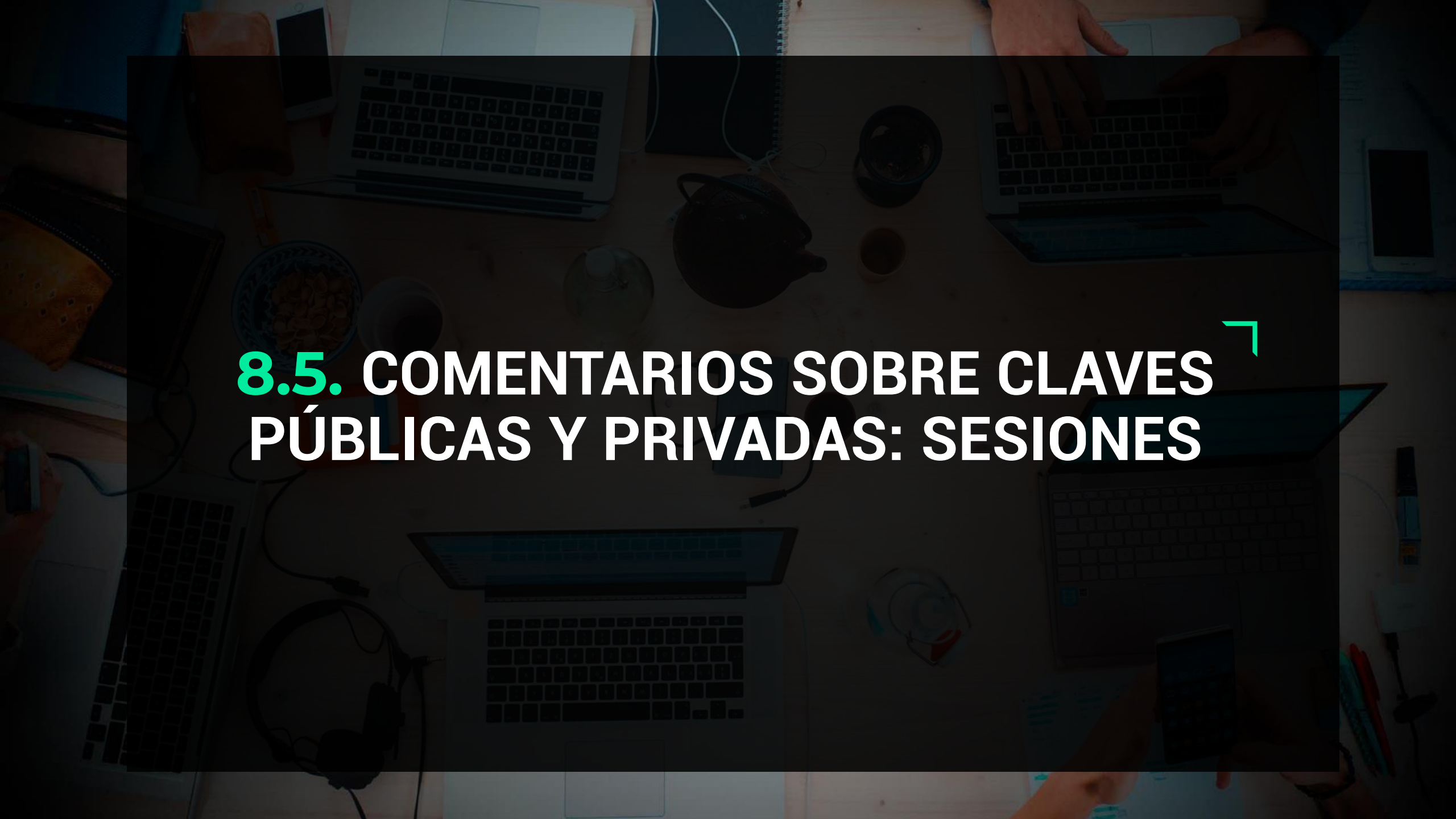
Mientras que las trasposiciones y las sustituciones pueden ser establecidas de forma sencilla, este tipo de criptografía necesita de procedimientos más complejos.

Pasado

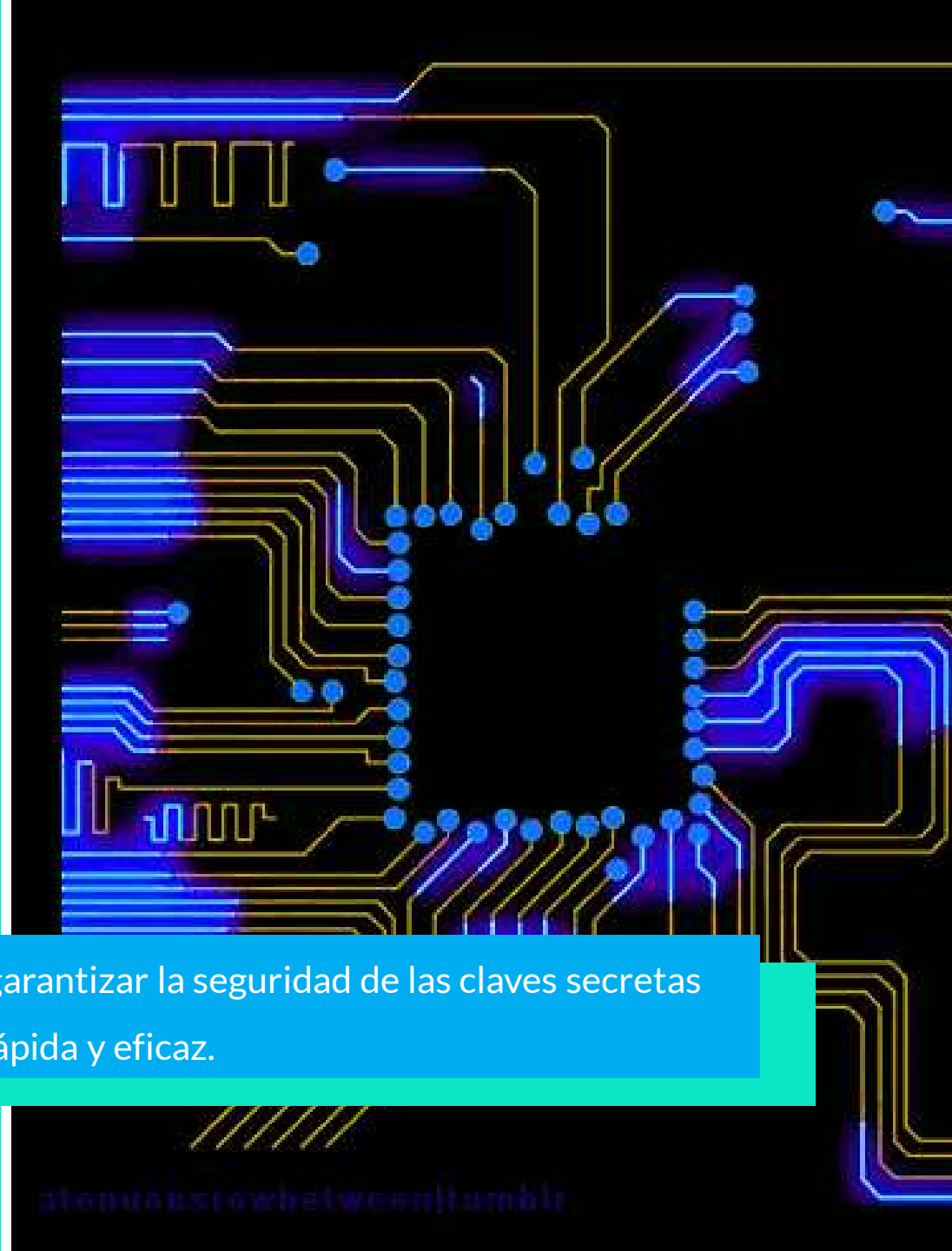
La **criptografía tradicional** se centraba en encontrar algoritmos que fuesen simples y claves largas para aumentar la seguridad.

Presente

Actualmente **los nuevos algoritmos** han desarrollado cifrados extremadamente complejos y con unas enormes cantidades de texto, que permiten **mejorar la seguridad** ampliamente con respecto a sus predecesores.



8.5. COMENTARIOS SOBRE CLAVES PÚBLICAS Y PRIVADAS: SESIONES



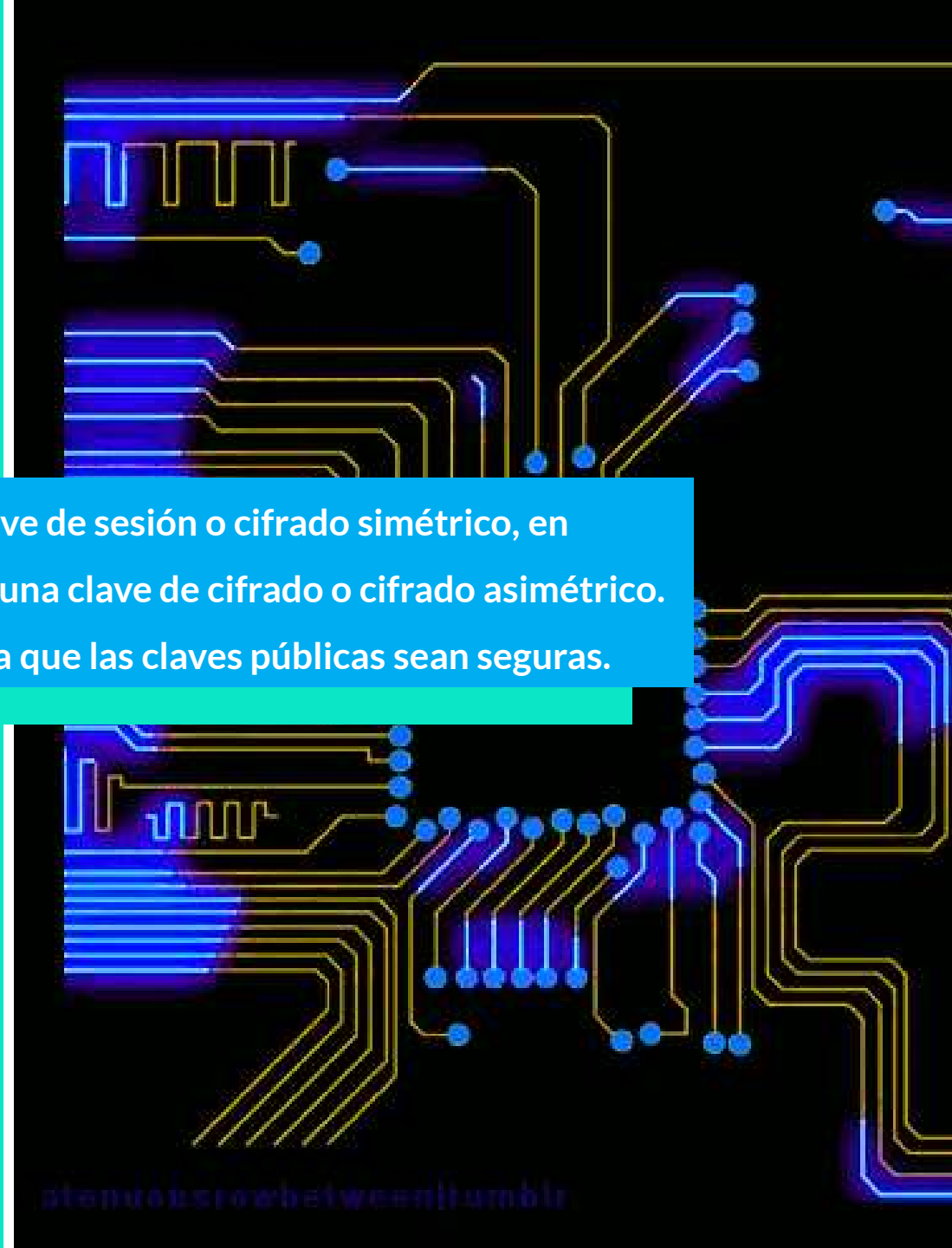
Cifrado simétrico

El tráfico de datos se suele cifrar usando la criptografía de **clave secreta** que es denominada como la "**clave de sesión o cifrado simétrico".**

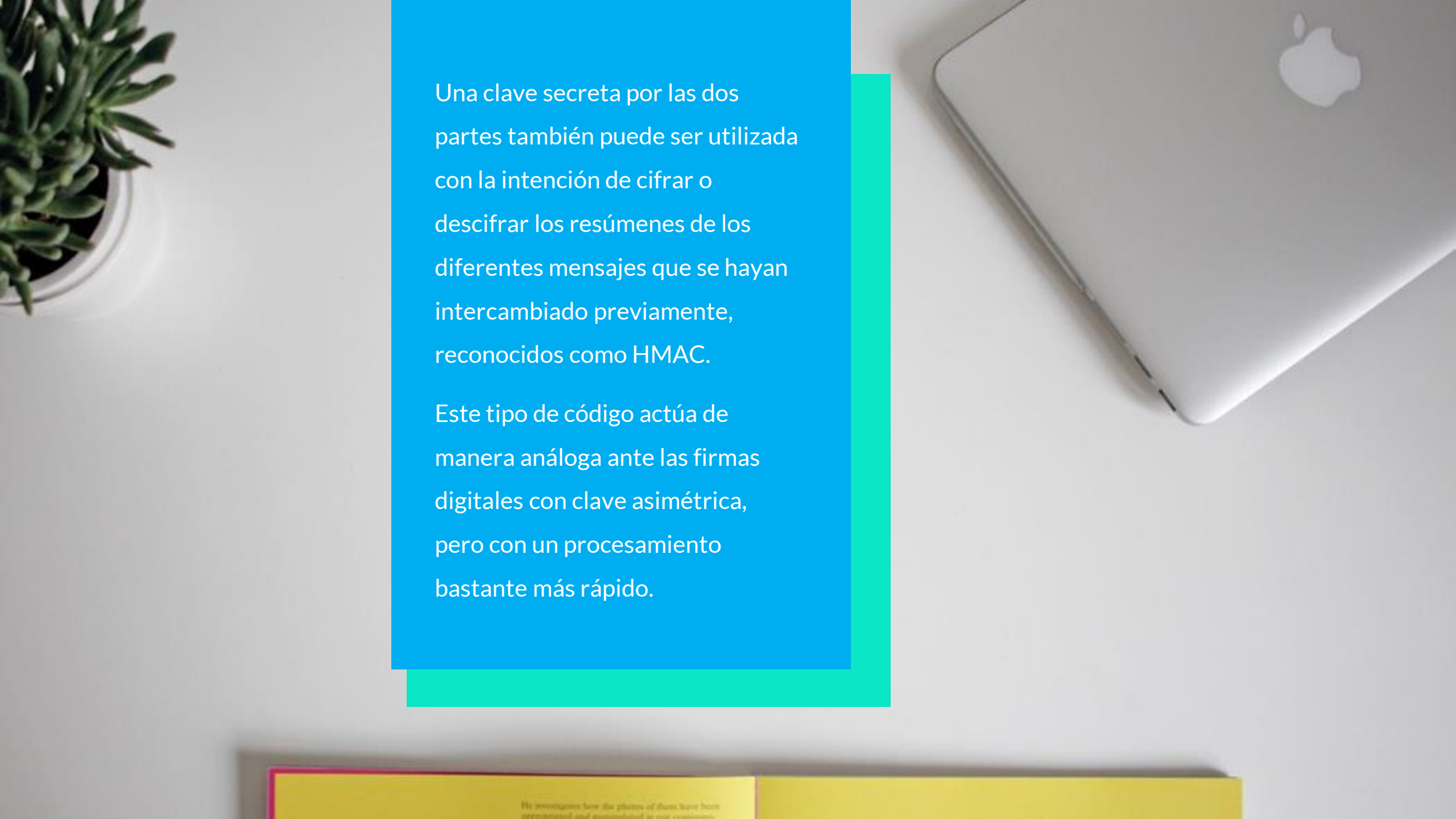
Cifrado asimétrico

La criptografía de **clave pública** se suele utilizar para crear una "**clave de sesión o cifrado asimétrico**".

La mezcla de los asimétricos es la que mejor funcionará para garantizar la seguridad de las claves secretas para cifrar la información de manera simétrica de forma más rápida y eficaz.



Para favorecer la velocidad y la seguridad, se utilizará la clave de sesión o cifrado simétrico, en cambio la criptografía de clave pública se utiliza para crear una clave de cifrado o cifrado asimétrico. Así, se podrá gestionar una clave secreta nueva que permita que las claves públicas sean seguras.



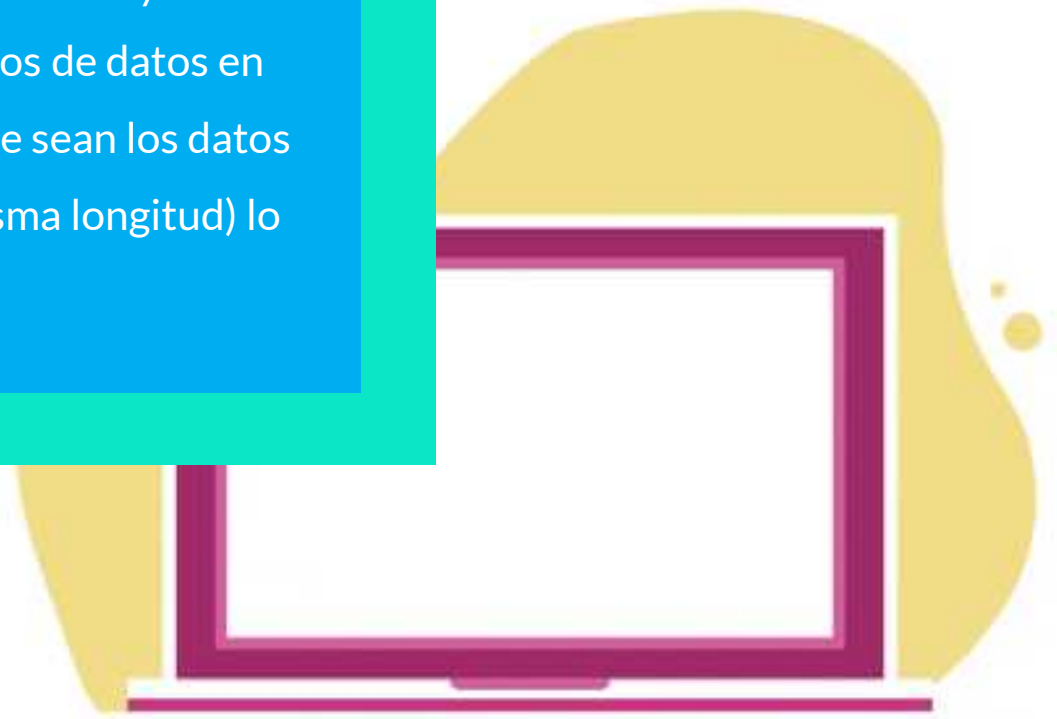
Una clave secreta por las dos partes también puede ser utilizada con la intención de cifrar o descifrar los resúmenes de los diferentes mensajes que se hayan intercambiado previamente, reconocidos como HMAC.

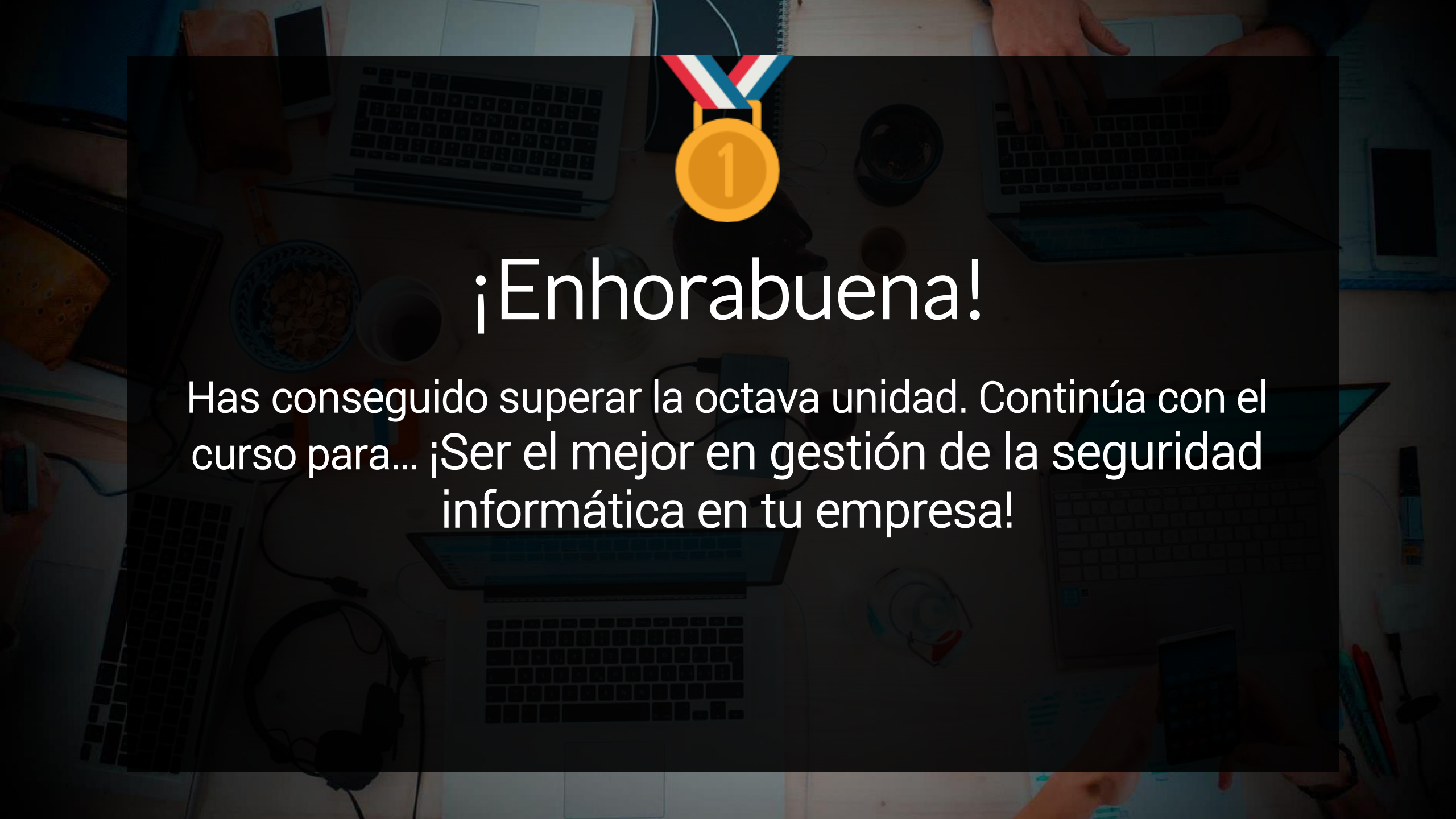
Este tipo de código actúa de manera análoga ante las firmas digitales con clave asimétrica, pero con un procesamiento bastante más rápido.

¿Qué se consigue con estas técnicas?

Mantener las comunicaciones para garantizar la confidencialidad y la autenticidad de los mensajes.

Ante la duda, siempre será mejor utilizar las longitudes de clave y *hash* (algoritmo matemático que transforma bloques arbitrarios de datos en nuevos caracteres con una longitud fija. Cualesquiera que sean los datos de entrada, el valor hash de salida, siempre, tendrá la misma longitud) lo más largas que se pueda.





¡Enhorabuena!

Has conseguido superar la octava unidad. Continúa con el curso para... ¡Ser el mejor en gestión de la seguridad informática en tu empresa!